

# IAD.GOV, IOSS.GOV, CNSS.GOV Users must install DoD Root Certificates by 24 February 2022

**IMPORTANT** On 24 February 2022 in order to access websites on the above domains, all users must install a DoD Root Certificate in their browser. You do not need to be affiliated with DoD to install these certificates. Guidance from the DISA webpage:

## In this document, we answer:

- How do I install DoD Root Certificates?
- How do you know if you already have the DoD Root Certs installed in your browsers? **CHECK THIS FIRST!**
  - o Chrome
  - o IE
  - o Firefox
  - o Edge
- What does it look like NOT to have DoD Root Certificates installed?

---

## *How do I to install DoD Root Certificates?*

---

In order for your machine to recognize DoD websites as trusted, run the InstallRoot utility to install the DoD CA certificates on Microsoft operating systems:

- **32-bit** ([https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/msi/InstallRoot\\_5.5x32.msi](https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/msi/InstallRoot_5.5x32.msi))
- **64-bit** ([https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/msi/InstallRoot\\_5.5x64.msi](https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/msi/InstallRoot_5.5x64.msi))
- **or Non Administrator** ([https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/msi/InstallRoot\\_5.5x32\\_NonAdmin.msi](https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/msi/InstallRoot_5.5x32_NonAdmin.msi))

If you're running an alternate operating system such as Mac OS or Linux, you can import certificates from the **PKCS 7 bundle** ([https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/zip/certificates\\_pkcs7\\_DoD.zip](https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/zip/certificates_pkcs7_DoD.zip)).

The **InstallRoot User Guide** is available at [https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/pdf/unclass-rg-installroot\\_5\\_2\\_niprnet\\_user\\_guide.pdf](https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/pdf/unclass-rg-installroot_5_2_niprnet_user_guide.pdf).

---

## *How do you know if you already have the DoD Root Certs installed in your browsers?*

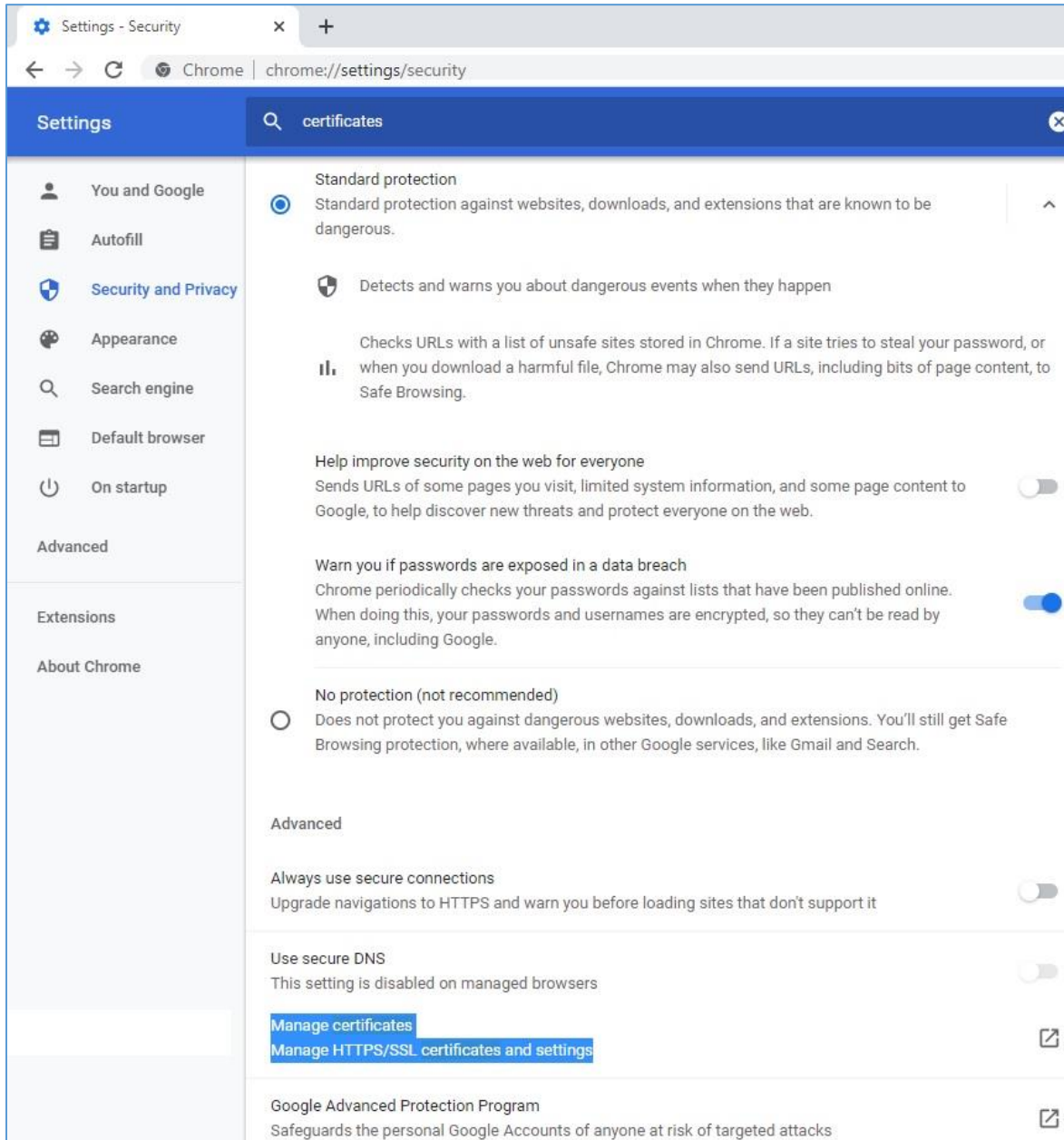
---

Follow the instructions below for each browser. You will need to look for an unexpired **DoD Root CA**.

## Chrome

Navigate to the URL: `chrome://settings/security` in Chrome.

Scroll down. Click **Manage Certificates** option.



A popup box called **Certificates** appears. Click the tab called **Trusted Root Certification Authorities**.

Scroll down and look for **DoD Root CA**.

**If you find it and it has not expired, you have the DoD Root Certificates installed! You have no further action to take.**

If you do not find any DoD Root CA listed or you find expired entries only, please follow the instructions above to download them.

# Certificates



Intended purpose:

<All>



Intermediate Certification Authorities

Trusted Root Certification Authorities

Trusted Publ



Issued To	Issued By	Expiratio...	Friendly Name
DigiCert High Assur...	DigiCert High Assuran...	11/9/2031	DigiCert
DigiCert Trusted Ro...	DigiCert Trusted Root...	1/15/2038	DigiCert Trusted ...
DoD CLASS 3 Root CA	DoD CLASS 3 Root CA	5/14/2020	<None>
DoD Root CA 2	DoD Root CA 2	12/5/2029	<None>
DoD Root CA 3	DoD Root CA 3	12/30/2029	<None>
DST Root CA X3	DST Root CA X3	9/30/2021	DST Root CA X3
Entrust Root Certifi...	Entrust Root Certifica...	11/27/2026	Entrust
Entrust Root Certifi...	Entrust Root Certifica...	12/7/2030	Entrust.net
Entrust.net Certific...	Entrust.net Certificati...	7/24/2029	Entrust (2048)

Import...

Export...

Remove

Advanced

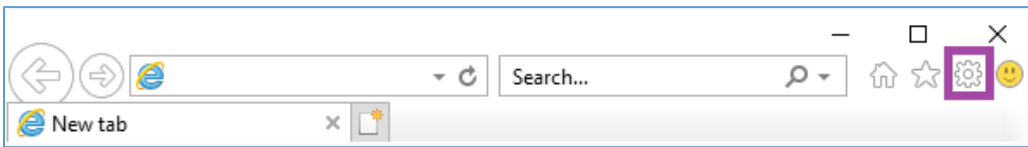
Certificate intended purposes

View

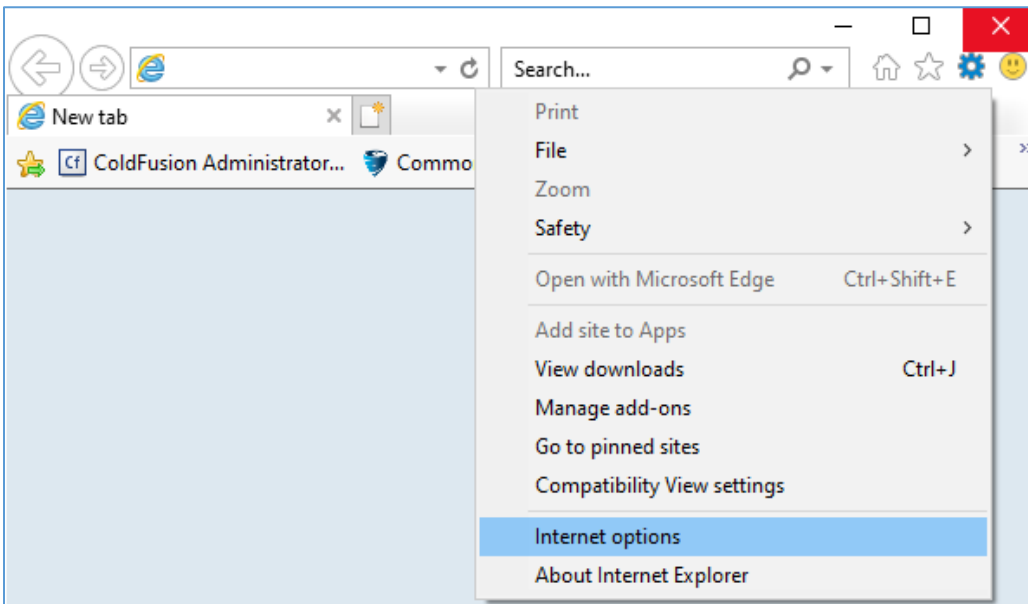
Close

## Internet Explorer (IE)

Click on the gear icon in the upper right corner of the browser.



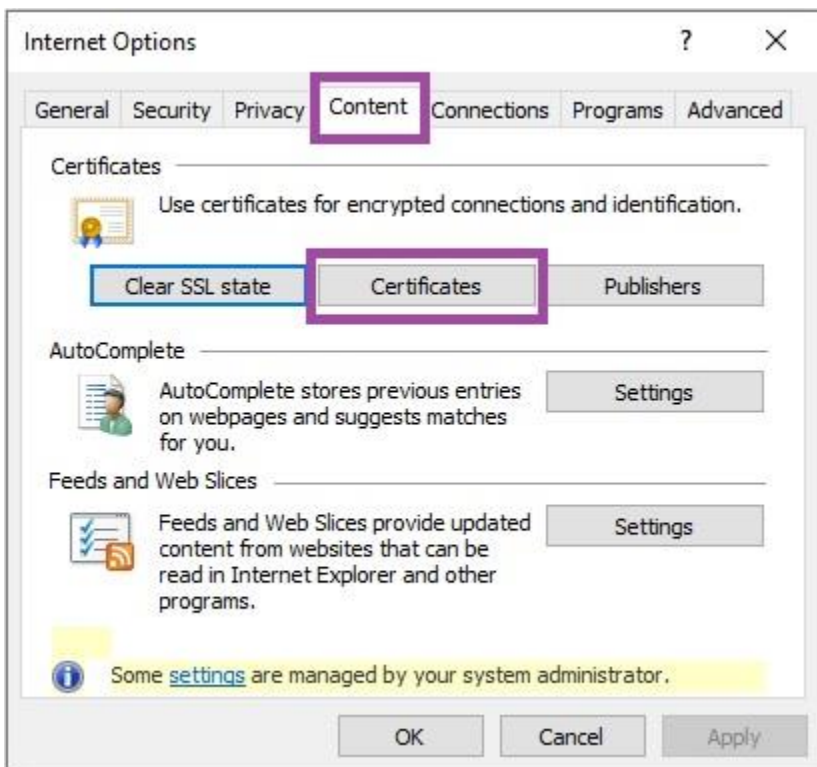
A list of options appears. Click **Internet Options**.

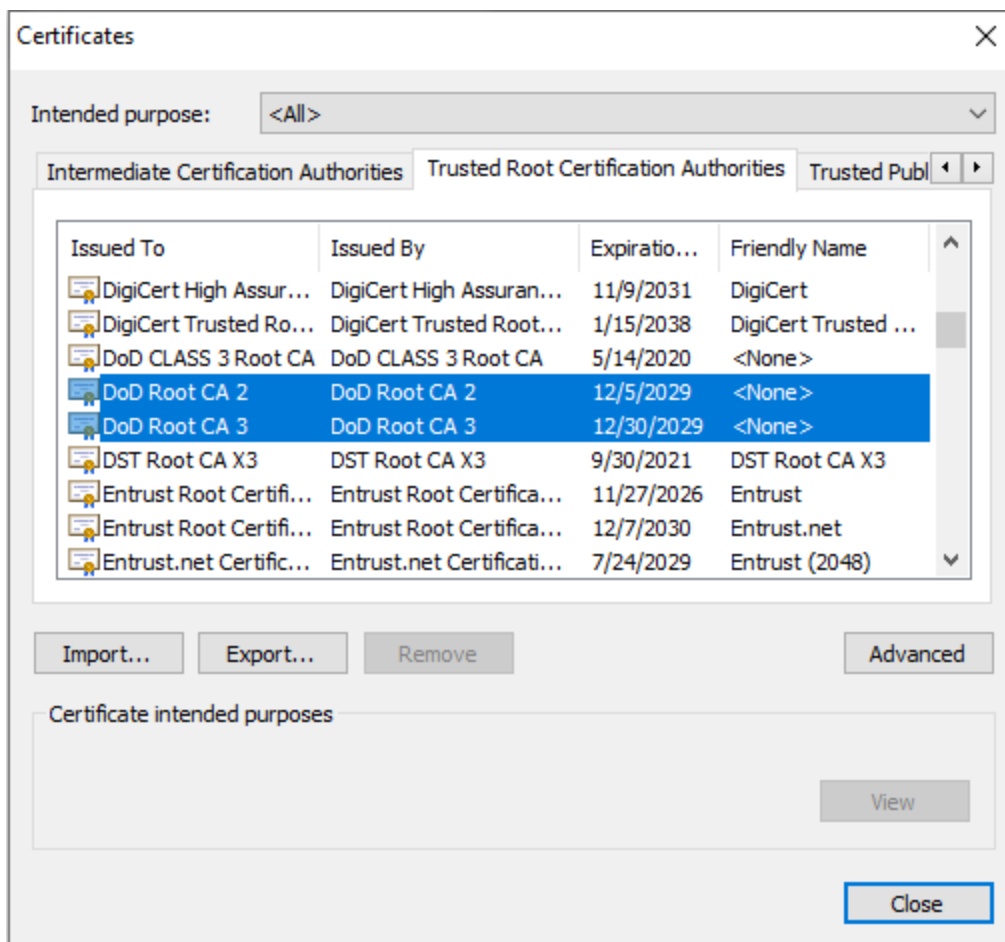


An **Internet Options** popup appears.

Click on the **Content** tab. Click on the **Certificates** button.

A popup box called **Certificates** appears. Click the tab called **Trusted Root Certification Authorities**.





Scroll down and look for **DoD Root CA**.

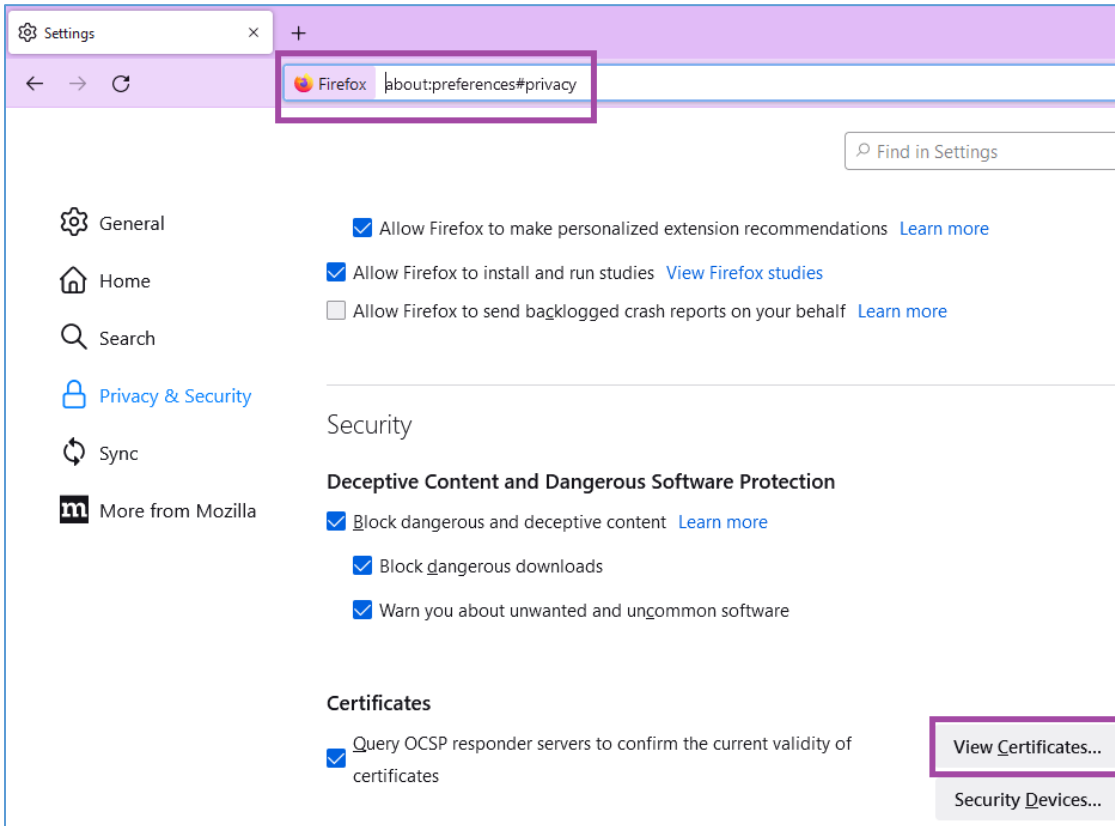
**If you find it and it has not expired, you have the DoD Root Certificates installed! You have no further action to take.**

If you do not find any DoD Root CA listed or you find expired entries only, please follow the instructions above to download them.

## Firefox:

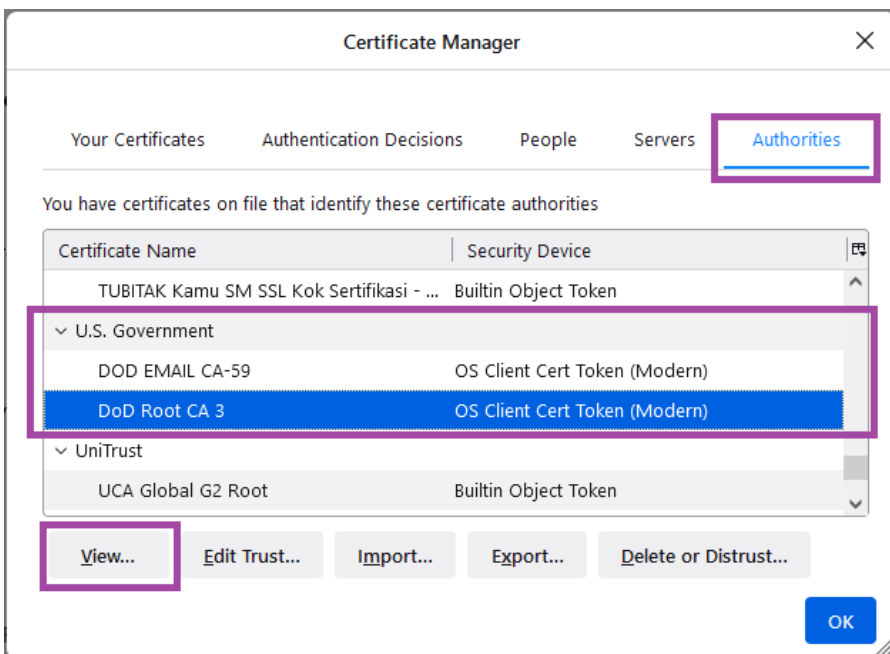
Navigate to the URL: **about:preferences#privacy** in Firefox.

Scroll down and click **View Certificates...** button.

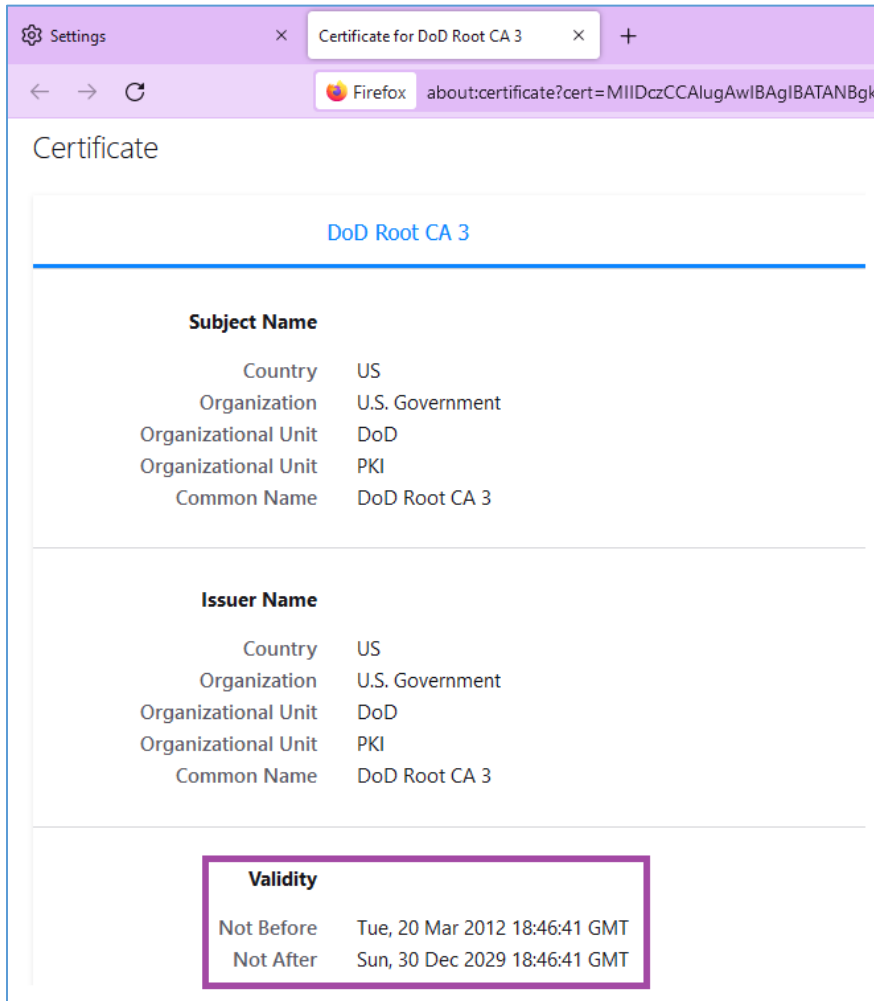


A popup called **Certificate Manager** appears. Click **Authorities** from the top row of choices.

Scroll down to find **U.S. Government** and then find **DoD Root CA**.



To be sure it isn't expired, click on **DoD Root CA**. The **View** button at the bottom of the popup becomes enabled. Click the **View** button.



The screenshot shows a Firefox browser window with the address bar displaying 'about:certificate?cert=MIIDczCCAlugAwIBAgIBATANBgk'. The page title is 'Certificate for DoD Root CA 3'. The main content area is titled 'Certificate' and displays the details for 'DoD Root CA 3'.

**Subject Name**

Country	US
Organization	U.S. Government
Organizational Unit	DoD
Organizational Unit	PKI
Common Name	DoD Root CA 3

**Issuer Name**

Country	US
Organization	U.S. Government
Organizational Unit	DoD
Organizational Unit	PKI
Common Name	DoD Root CA 3

**Validity**

Not Before	Tue, 20 Mar 2012 18:46:41 GMT
Not After	Sun, 30 Dec 2029 18:46:41 GMT

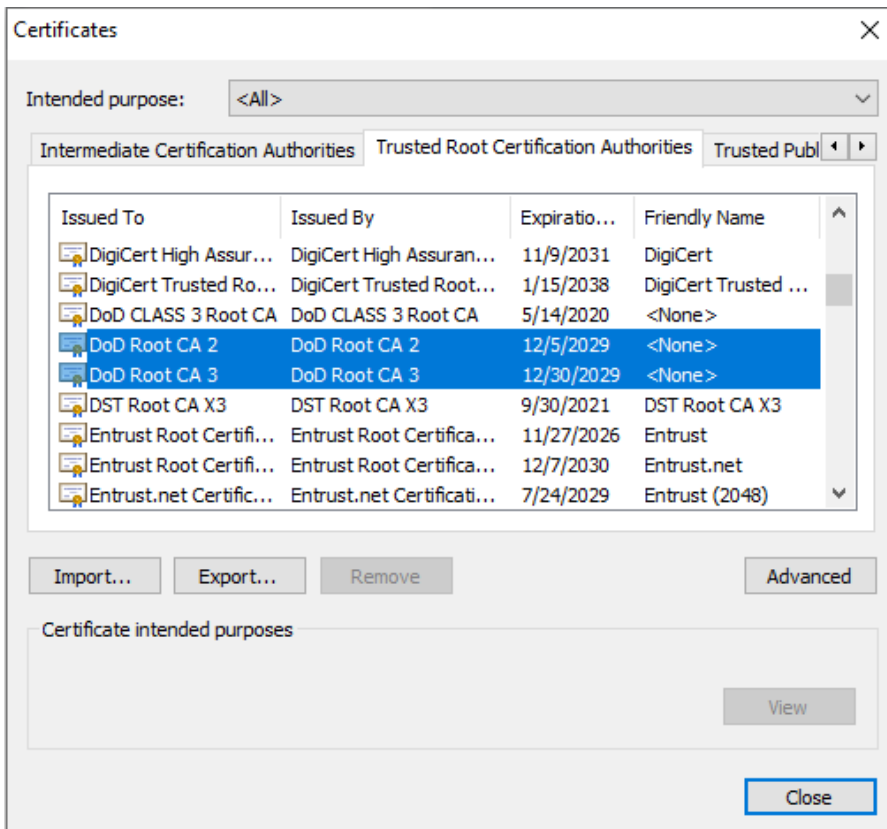
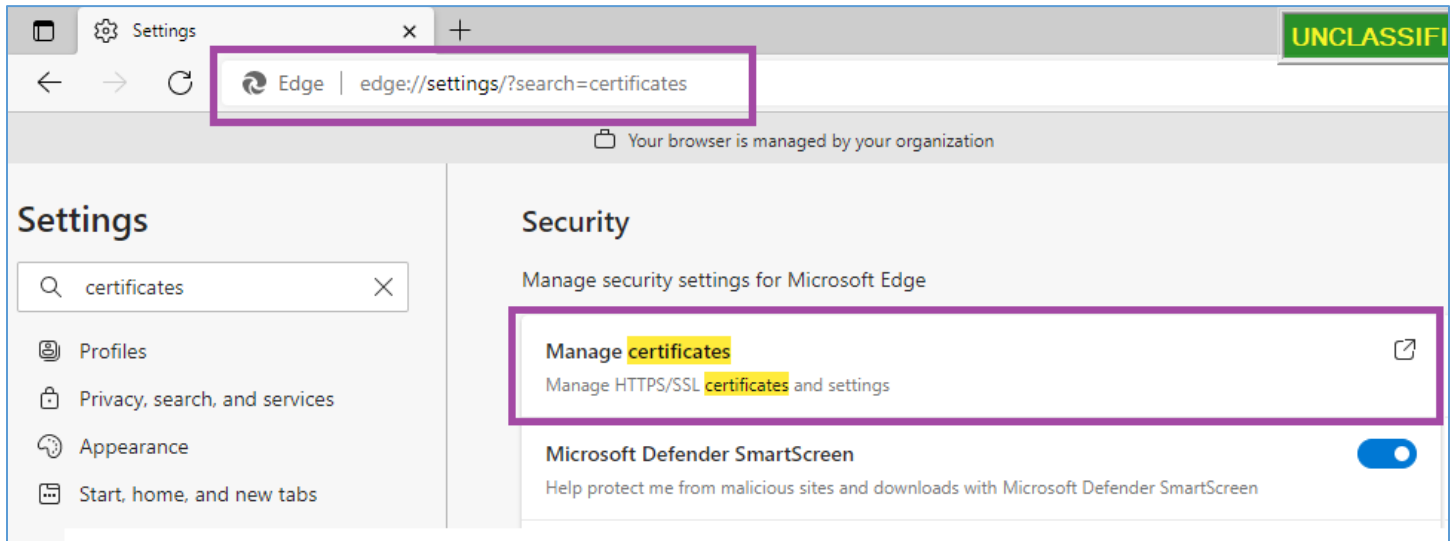
Certificate information opens in a new tab. Look for the Validity section to find if the root certificate is expired.

**If you find it and it has not expired, you have the DoD Root Certificates installed! You have no further action to take.**

## Edge

Navigate to the URL: **edge://settings/?search=certificates** in Edge.

Click **Manages Certificates** option.



A popup box called **Certificates** appears. Click the tab called **Trusted Root Certification Authorities**.

Scroll down and look for **DoD Root CA**.

**If you find it and it has not expired, you have the DoD Root Certificates installed! You have no further action to take.**

If you do not find any DoD Root CA listed or you find expired entries only, please follow the instructions above to download them.



---

## What does it look like NOT to have DoD Root Certificates Installed?

---

It varies by browser, but it will look similar to the following screenshot.

Currently, some browsers allow you to bypass the security warning by clicking **Advanced** and accepting the risk.

**However, on 24 February 2022, the bypass option will likely not be available for these sites.**

The screenshot shows a Firefox browser window with a purple header bar. The address bar displays a warning icon, the text 'Warning: Potential Security Risk', and a close button. Below the address bar, the page title is 'Warning: Potential Security Risk Ahead' next to an orange warning triangle icon. The main content area explains that Firefox detected a potential security threat and did not continue to the website. It provides instructions on what to do about it, including checking for updates or contacting the website administrator. At the bottom, there are two buttons: 'Go Back (Recommended)' and 'Advanced...'. A green arrow points down from the 'Advanced...' button to a detailed warning box. This box contains the text: 'Someone could be trying to impersonate the site and you should not continue.', 'Websites prove their identity via certificates. Firefox does not trust www.iad.gov because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.', and the error code 'SEC\_ERROR\_UNKNOWN\_ISSUER'. There is a 'View Certificate' link and another 'Go Back (Recommended)' button. A black box with red text is overlaid on the bottom right of the detailed warning box, stating: 'Accept the Risk and Continue likely not an option after 2/24/2022'. At the bottom of the browser window, there are two buttons: 'Go Back (Recommended)' and 'Accept the Risk and Continue'.

Warning: Potential Security Risk X

← → ↻ Not Secure https://www.iad.gov/iad/

### Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to www.iad.gov. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

**What can you do about it?**

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

Go Back (Recommended) Advanced...

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust www.iad.gov because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC\_ERROR\_UNKNOWN\_ISSUER

[View Certificate](#)

Go Back (Recommended) Accept the Risk and Continue

**"Accept the Risk and Continue" likely not an option after 2/24/2022**